

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,610	07/26/2001	Chris A. Barton	NAIIP021/01.138.01	8705
28875	7590	08/18/2004	EXAMINER BAUM, RONALD	
SILICON VALLEY INTELLECTUAL PROPERTY GROUP P.O. BOX 721120 SAN JOSE, CA 95172-1120			ART UNIT 2136	PAPER NUMBER

DATE MAILED: 08/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/916,610

Applicant(s)

BARTON ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☒ Claim(s) 8 and 17 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 1/12/01, 1/23/03
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_

### **DETAILED ACTION**

1. Claims 1-24 are pending for examination.
2. Claims 1-24 are rejected.

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8,17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "proprietary" in claims 8,17 is a relative term which renders the claim indefinite. The term "proprietary" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the sake of applying art, the examiner will take the broadest interpretation of the term to encompass any manufactured item by said manufacturer.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2136

3. Claims 1-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Hill et al, U.S. Patent 6,088,804.

4. As per claim 1; “A method for scanning data utilizing multiple scanning engines [figure 1 and accompanying description], comprising: (a) generating a request for data to be scanned for viruses utilizing a scanning interface [col. 4, lines 5-col. 10, line 4, whereas the “processor in communication with the security agents... [col. 3, lines 17-40]” constitute a scanning interface]; (b) sending the request to scan data to a plurality of scanning engines utilizing an engine interface application control module coupled between the scanning interface and the scanning engines, the request being adapted for prompting the scanning engines to scan the data and respond with events upon locating a virus [col. 4, lines 5-col. 10, line 4, whereas the creation of the signatures to be subsequently used by the agents constitutes requests to the scanning engines]; (c) receiving the events utilizing an event processor module coupled to the scanning engines and the engine interface application control module for processing the events [col. 4, lines 5-col. 10, line 4, whereas the signatures subsequently used by the agents to scan, producing said scanner results that are forwarded back to the display/network management node, constitutes “receiving the events” resulting from requests to the scanning engines. Further, the SOM processor in the ANN security system architecture clearly addresses the engine interface application control module functionality.]; and (d) transmitting the processed events to the engine interface application control module for being monitored by the scanning interface [col. 4, lines 5-col. 10, line 4, whereas the scanner results that are forwarded back to the display/network management node, constitutes “monitored by the scanning interface” resulting from scanner results that are forwarded back.].”;

Art Unit: 2136

Further, as per claim 10; “A computer program product [This claim is the software computer-readable medium claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for scanning data utilizing multiple scanning engines, comprising: (a) computer code for generating a request for data to be scanned for viruses utilizing a scanning interface; (b) computer code for sending the request to scan data to a plurality of scanning engines utilizing an engine interface application control module coupled between the scanning interface and the scanning engines, the request being adapted for prompting the scanning engines to scan the data and respond with events upon locating a virus, (c) computer code for receiving the events utilizing an event processor module coupled to the scanning engines and the engine interface application control module for processing the events; and (d) computer code for transmitting the processed events to the engine interface application control module for being monitored by the scanning interface.”;

Further, as per claim 20; “A system [This claim is the apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for scanning data utilizing multiple scanning engines, comprising: (a) a scanning interface for generating a request for data to be scanned for viruses; (b) an engine interface application control module coupled between the scanning interface and a plurality of scanning engines for sending the request to scan data to the scanning engines, the request being adapted for prompting the scanning engines to scan the data and respond with events upon locating a virus; and (c) an event processor module coupled to the scanning engines and the engine interface application control module for receiving the events and processing the events; (d) wherein the processed events are outputted by the scanning interface.”;

Art Unit: 2136

Further, as per claim 21; “A method [This claim is the method/means claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for scanning data utilizing multiple scanning engines, comprising: (a) means for generating a request for data to be scanned for viruses; (b) means for sending the request to scan data to the scanning engines, the requests being adapted for prompting the scanning engines to scan the data and respond with events upon locating a virus; and (c) means for receiving the events and processing the events. ”.

5. Claim 2 ***additionally recites*** the limitation that; “The method as recited in claim 1 wherein the engine interface application control module and the event processor module reside on a gateway.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the “... Security system 20 functions in conjunction with existing technologies for intrusion detection and other network attack recognition techniques. Most security events are defeated at the *node level* by the existing technologies such as by *protection software and systems like firewalls and filters*... [col. 4, lines 30-60]”, and further, the SOM processor in the ANN security system architecture clearly addresses the peripheral network node (i.e., gateway node of a network input/output) functionality.);

Further, as per claim 11 ***additionally reciting*** the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] as recited in claim 10, wherein the engine interface application control module and the event processor module reside on a gateway.”.

Art Unit: 2136

6. Claim 3 ***additionally recites*** the limitation that; “The method as recited in claim 2, wherein the scanning interface automatically generates the request in response to the receipt of data at the gateway.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the “...Most security events are defeated at the *node level* by the existing technologies such as by *protection software and systems like firewalls and filters*... [col. 4, lines 30-60]”, and further, the SOM processor in the ANN security system architecture clearly addresses the peripheral network node (i.e., gateway node of a network input/output) functionality, and further initiate the learning cycle/node signature update (i.e., request scanning after node update for subsequent attack detection based on attack signature));

Further, as per claim 12 ***additionally reciting*** the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] as recited in claim 11, wherein the scanning interface automatically generates the request in response to the receipt of data at the gateway.”.

7. Claim 4 ***additionally recites*** the limitation that; “The method as recited in claim 1, wherein the scanning interface includes a graphical user interface for allowing a user to manually generate the request.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the SOM processor and associated display/display processor in the ANN security system architecture clearly addresses the GUI network node (i.e., gateway node of a network input/output) functionality, and further initiate the learning cycle/node signature update manually under user control.);



Art Unit: 2136

Further, as per claim 13 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] as recited in claim 10, wherein the scanning interface includes a graphical user interface for allowing a user to manually generate the request.”.

8. Claim 5 *additionally recites* the limitation that; “The method as recited in claim 1, wherein the engine interface application control module translates the requests for each of the scanning engines.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the SOM processor and associated display/display processor in the ANN security system architecture clearly addresses the forwarding of signature updates (i.e., request to scan with updated attack signature) functionality, and further initiate the learning cycle/node signature update to the security agents.);

Further, as per claim 14 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection] as recited in claim 10, wherein the engine interface application control module translates the requests for each of the scanning engines.”.

9. Claim 6 *additionally recites* the limitation that; “The method as recited in claim 1, wherein the event processor module translates the events from each of the scanning engines into a single format.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4,

Art Unit: 2136

whereas the SOM processor and associated display/display processor in the ANN security system architecture clearly addresses the forwarding of results of the scans resulting from previously forwarding of signature updates (i.e., request to scan with updated attack signature) functionality. Further, the common network communications protocol (i.e., TCP/IP in the Internet case of FTP requests) addresses the commonality of interface protocol, inasmuch as all nodes involved are part of a network that can communicate on a node to node basis.);

Further, as per claim 15 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] as recited in claim 10, wherein the event processor module translates the even-s from each of the scanning engines into a single format.”.

10. Claim 7 *additionally recites* the limitation that; “The method as recited in claim 6, wherein the translated events are transmitted to the scanning interface for outputting the event.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the SOM processor and associated display/display processor in the ANN security system architecture clearly addresses the forwarding of results of the scans and subsequent rendering (i.e., the GUI).);

Further, as per claim 16 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection] as recited in claim

Art Unit: 2136

15 wherein the translated events are transmitted to the scanning interface for outputting the event.”.

11. Claim 8 *additionally recites* the limitation that; “The method as recited in claim 1, wherein the scanning engines are proprietary scanning engines.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas for the sake of applying art, the scanning engines are clearly proprietary, relative to whoever manufactured the specific engine used. Further, since the Hill et al ANN security scanners are recited as “existing technologies...”, the scanners are clearly inherently proprietary.);

Further, as per claim 17 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection] as recited in claim 10, wherein the scanning engines are proprietary scanning engines.”.

12. Claim 9 *additionally recites* the limitation that; “The method as recited in claim 1, wherein the scanning engines are incompatible scanning engines.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas for the sake of applying art, the scanning engines are clearly incompatible in the sense that the scanning engines of Hill et al are taught before they scan. Therefore, the attack signature, which is an inherent part of the scan functionality upon the said attack data update to the security agents, having been created as a function of the network topology during the learning phase, makes each agent unique as far as the scan profile used to create a scan result to be forwarded back for rendering );

Art Unit: 2136

Further, as per claim 18 *additionally reciting* the limitation that; “The computer program product [This claim is the software computer-readable medium claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection] as recited in claim 10, wherein the scanning engines are incompatible scanning engines.”.

13. Claim 19 *additionally recites* the limitation that; “The computer program product as recited in claim 10, wherein the events include the identification of at least one of unwanted content, viruses and malicious code.”. The teachings of Hill et al suggest such limitations (col. 4, lines 5-col. 10, line 4, whereas the scanning engines clearly send back results which are inherently an identification of the fact that the scan resulted in finding something associated with what the scanning agent was taught by the attack signature (i.e., a signature of an attack by a worm, virus, generally malicious malware, etc.) it was updated with subsequent to the scan. Therefore, the attack signature, which is an inherent part of the scan functionality upon the said attack data update to the security agents, having been created as a function of the network topology during the learning phase, makes each agent unique as far as the scan profile used to create a scan result to be forwarded back for rendering.).

14. As per claim 22; “A method for scanning data utilizing multiple scanning engines, comprising: (a) receiving data at a gateway [col. 4, lines 5-col. 10, line 4, see claim 2 rejection above]; (b) generating a request for the data to be scanned for viruses in response to the receipt of data at the gateway utilizing a scanning interface [col. 4, lines 5-col. 10, line 4, see claim 2 rejection above]; (c) translating the request utilizing an engine interface application control

Art Unit: 2136

module coupled between the scanning interface and a plurality of scanning engines [col. 4, lines 5-col. 10, line 4, see claim 2 rejection above]; (d) sending the translated request to the scanning engines utilizing the engine interface application control module, the request being adapted for prompting the scanning engines to scan the data and respond with events upon locating a virus [col. 4, lines 5-col. 10, line 4, see claims 1, 2 rejections above]; (e) receiving the events utilizing an event processor module coupled to the scanning engines and the engine interface application control module [col. 4, lines 5-col. 10, line 4, see claim 1 rejections above]; (f) checking an integrity of the events received utilizing the event processor module [col. 4, lines 5-col. 10, line 4, see claim 6 rejection above, whereas the use of TCP/IP Internet protocol (i.e., for "...FTP requests...") inherently encompasses the use of packet integrity checking.]; (g) translating the events into a common format utilizing the event processor module if the events pass the integrity check engines [col. 4, lines 5-col. 10, line 4, see claim 6 rejection above]; (h) transmitting the translated events to the engine interface application control module [col. 4, lines 5-col. 10, line 4, see claim 1 rejections above]; and (i) outputting the translated events utilizing the scanning interface [col. 4, lines 5-col. 10, line 4, see claim 1 rejections above].".

15. As per claim 23; "A method for scanning data utilizing a system capable of interfacing multiple scanning engines, comprising: identifying a request from a user for data to be scanned for viruses utilizing an interface [col. 4, lines 5-col. 10, line 4, see claims 1, 2 rejections above]; translating the request to be utilized by at least one of a plurality of different scanning engines [col. 4, lines 5-col. 10, line 4, see claims 1, 2, 5 rejections above]; sending the translated request to the at least one of the scanning engines, the request being adapted for prompting the at least one scanning engine to scan the data and respond with events upon locating a virus [col. 4, lines 5-

Art Unit: 2136

col. 10, line 4, see claims 1, 2 rejections above]; receiving the events from the at least one scanning engine [col. 4, lines 5-col. 10, line 4, see claim 1 rejections above]; translating the events into a common format [col. 4, lines 5-col. 10, line 4, see claim 7 rejections above]; and outputting the translated events utilizing the interface [col. 4, lines 5-col. 10, line 4, see claim 1, 6, 7 rejections above].”;

Further, as per claim 24 *additionally reciting* the limitation that; “A computer program product [This claim is the software computer-readable medium claim for the method claim 23 above, and is rejected for the same reasons provided for the claim 23 rejection] for scanning data utilizing a system capable of interfacing multiple scanning engines, comprising: computer code for identifying a request from a user for data to be scanned for viruses utilizing an interface; computer code for translating the request to be utilized by at least one of a plurality of different scanning engines; computer code for sending the translated request to the at least one of the scanning engines, the request being adapted for prompting the at least one scanning engine to scan the data and respond with events upon locating a virus; computer code for receiving the events from the at least one scanning engine; computer code for translating the events into a common format; and computer code for outputting the translated events utilizing the interface.”.

### ***Conclusion***

16. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

Art Unit: 2136

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:


After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7246

Ronald Baum

Patent Examiner

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100